Vereinbarung zur Auftragsverarbeitung

zwischen

Scheibenkalkulator- Nutzer
nachfolgend „Auftraggeber“ genannt

und der

Adolf Würth GmbH & Co. KG
Reinhold- Würth- Straße 12-17
74653 Künzelsau- Gaisbach -

-

nachfolgend „Auftragnehmer“ genannt

gemeinsam nachfolgend „Parteien“ genannt

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Akzeptanz der Nutzungsbedingungen (Leistungsvereinbarung) zwischen dem Auftraggeber und dem Auftragnehmer, auf die hier verwiesen wird (im Folgenden „Leistungsvereinbarung“).

1.2. Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

- Gegenstand des Vertrages ist das Softwarehosting und der Support des webbasierten Scheibenkalkulator Abrechnungssystems, welches der Auftraggeber und gegebenenfalls seine Filialen zur Abwicklung von Glasschaden mit der Versicherungswirtschaft, oder seinen Kunden einsetzt.
- Die Glasschadendaten werden zum Teil online zur Abrechnung über definierte Schnittstellen, oder per Email, oder per Post versendet.
- Entgegennahme von Bestellprozessen zur Verarbeitung bei Teilehändlern, Glasgroßhändlern

- Statistikdaten zur Verarbeitung bei den Franchisegebern, Zentralen der Werkstatt-Gruppen und Zentralen von Werkstattkonzepten

Zum Zweck der vertraglich vereinbarten Erbringung der Leistung und deren Abrechnung werden in unserem House darüber hinaus folgende Daten verarbeitet.

- Vertragsdaten, Produktdaten, Kundenstammdaten, Zahlungsdaten zur Rechnungslegung der Werkstätten
- Protokollierung der durchgeführten Maßnahmen im Helpdesk zur Erfüllung der vertraglich vereinbarten Dienstleistungen im Rahmen der Störungsbeseitigung, Beratung.
- Infomailings zu Störungsbeseitigungen, Updates und allgemeinen Informationen
- Erstellen von Angeboten

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2.2. Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien: (Aufzahlung/Beschreibung der Datenkategorien) z.B.:

- Personenstammdaten
- Versicherungsdaten
- Schadensdaten, Schadensbilder
- Fahrzeugdaten, Fahrzeugbilder
- Glasschaden- Kalkulationsdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Daten zu Störungsmeldungen und deren Beseitigung
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

2.3. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Werkstätten
- Werkstattkunden
- Interessenten
- Beschäftigte
- Lieferanten
- Handelsvertreter

- Ansprechpartner
- Teilehändler

3. Technische und organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Einzelheiten in der Anlage „Technische und organisatorische Maßnahmen". Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Anfragen und Rechte Betroffener

4.1. Der Auftragnehmer unterstützt den Auftraggeber in angemessener Weise bei der Erfüllung von dessen Pflichten nach Art. 12–22, 32 bis 36 DSGVO. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers herausgeben, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2. Der Auftraggeber stellt sicher, dass er die Informationspflichten gegenüber dem Betroffenen gemäß den Art. 12 ff. DSGVO erfüllt. Zusätzlich macht er, falls erforderlich, gegenüber dem Auftragnehmer Angaben, wie der Auftragnehmer die in den Art. 12 ff. DSGVO geforderten Informationen dem Betroffenen zur Verfügung stellen muss.

5. Datenschutzbeauftragter des Auftragnehmers

Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

6. Weitere Pflichten von Auftraggeber und Auftragnehmer

6.1. Der Auftragnehmer garantiert die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

6.2. Auftraggeber und Auftragnehmer vereinbaren die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO.

6.3. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Dies beinhaltet die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

6.4. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

6.5. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

7. Unterauftragsverhältnisse

7.1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

7.2. Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Würth IT GmbH	Industriepark Würth Drillberg 6 97980 Bad Mergentheim Deutschland	Auslagerung der IT-Systeme in das Rechenzentrum der Würth IT GmbH
Saint Gobain Autover Deutschland GmbH (Sekurit Service)	Boschstr 61-65 50171 Kerpen Deutschland	Softwarehosting und Support eines webbasierten Abrechnungssystems, welches zur Abwicklung von Glasschaden mit der Versicherungswirtschaft oder Kunden eingesetzt wird

7.3. Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht innerhalb von 30 (dreißig) Tagen nach Anzeige gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

Sofern der Auftraggeber aus datenschutzrechtlichen Gründen einen berechtigten Grund hat, der Verarbeitung personenbezogener Daten durch die neuen Unterauftragnehmer zu widersprechen, kann er die Vereinbarung durch schriftliche Erklärung gegenüber dem Auftragnehmer mit Wirkung zu einem vom Auftraggeber festgelegten Zeitpunkt kündigen, spätestens jedoch zum Ablauf von 30 (dreißig) Tagen nach dem Datum der Mitteilung durch den Auftragnehmer an den Auftraggeber über den neuen Unterauftragnehmer. Kündigt der Auftraggeber nicht innerhalb dieser Frist von dreißig (30) Tagen, so gilt der neue Unterauftragnehmer als durch den Auftraggeber genehmigt.

7.4. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

7.5. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der

Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Ziffer 7 Abs. 1 Satz 2 eingesetzt werden sollen.

8. Kontrollrechte des Auftraggebers

8.1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die mit angemessener Frist im Voraus anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

8.2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

8.3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

8.4. Kontrollen sind durch den Auftraggeber unter Einhaltung einer angemessenen Frist, mindestens jedoch 60 (sechzig) Tage im Voraus, anzukündigen.

8.5. Innerhalb eines Zeitraums von zwei Jahren ist der Auftraggeber zur Durchführung einer Kontrolle berechtigt, ohne dass der Auftragnehmer hierfür einen Vergütungsanspruch für die Bereitstellung von Personal geltend machen kann. Möchte der Auftraggeber weitere Kontrollen innerhalb dieses Zeitraums durchführen, kann der Auftragnehmer einen Vergütungsanspruch in Höhe von 125 € für jede Stunde geltend machen, in der der Auftragnehmer Personal zur Durchführung der Kontrolle bereitstellt.

8.6. In begründeten Einzelfällen, insbesondere bei wesentlichen Änderungen der Verarbeitungstätigkeit, den vereinbarten technischen und organisatorischen Maßnahmen oder datenschutzrelevanten Vorfällen, hat der Auftraggeber Anspruch auf weitere vergütungsfreie Kontrollen. Die Gründe hierfür sind durch den Auftraggeber anzuführen. Der Auftragnehmer berücksichtigt die Begründung des Auftraggebers bei der Entscheidung für die Ermöglichung weiterer vergütungsfreier Kontrollen in angemessener Weise.

9. Unterstützungspflichten des Auftragnehmers und Mitteilung bei Verstößen

9.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

9.2. Für Unterstützungsleistungen, die nicht in der Leistungsvereinbarung enthalten oder auf ein Fehlverhalten des Auftraggebers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10. Weisungsbefugnis des Auftraggebers

10.1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

10.2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11. Löschung und Rückgabe von personenbezogenen Daten

11.1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

11.2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

11.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12. Schlussbestimmungen

12.1. Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

12.2. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

12.3. Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt.

Künzelsau, 15.06.2025

Unterschrift Auftragnehmer

Anlage -
Technische und Organisatorische Maßnahmen (TOMS)
ADOLF WÜRTH GMBH & CO. KG

1. Zweck, Anwendungsbereich und Anwender

Organisationen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Sicherheit der Daten und damit einen wichtigen Teil der Einhaltung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.
Technische und organisatorische Maßnahmen werden in den Anforderungen des Datenschutzes methodisch geordnet. Diese Kategorien sind wie folgt unterteilt:

- **Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**
  - Zutrittskontrolle
  - Zugangskontrolle
  - Zugriffskontrolle
  - Trennungskontrolle
  - Pseudonymisierung
- **Integrität (Art. 32 Abs. 1 lit. b DSGVO)**
  - Weitergabekontrolle
  - Eingabekontrolle
- **Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**
  - Verfügbarkeitskontrolle
- **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)**
  - Datenschutz-Maßnahmen
  - Incident-Response-Management
  - Datenschutzfreundliche Voreinstellungen
  - Auftragskontrolle

Die o.g. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

2. Referenzdokumente

- ISO/IEC 27001 Standard
- 5.2 Richtlinie Informationssicherheit

3. Vertraulichkeit

3.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Automatisches Zugangskontrollsystem	☒ Empfang / Rezeption / Pförtner
☒ Biometrische Zugangssperren	☒ Besucherbuch / Protokoll der Besucher
☒ Chipkarten/Transpondersysteme	☒ Mitarbeiter- / Besucherausweise
☒ Manuelles Schließsystem	☒ Besucher in Begleitung durch Mitarbeiter
☒ Sicherheitsschlösser	☒ Sorgfalt bei Auswahl des Wachpersonals
☒ Absicherung der Gebäudeschächte	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Türen mit blindgeschalteter Klinke Außenseite	
☒ Klingelanlage mit Kamera	
☒ Videoüberwachung der Eingänge	
☒ Videoüberwachung im Innenbereich	
☒ Sicherheitsverglasung	

3.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die Verhinderung der unbefugten Nutzung von Anlagen gemeint.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzer + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Zertifikatbasierte Zugriffberechtigung	☒ Erstellen von Benutzerprofilen
☒ Anti-Viren-Software Server	☒ Zentrale Policy für Passwortvergabe (Wechseldauer, Komplexität)
☒ Anti-Virus-Software-Clients (Desktops, Laptops, Windows-Tablets)	☒ Besucherbuch / Protokoll der Besucher
☒ Firewall	☒ Mitarbeiter- / Besucherausweise
☒ Intrusion Prevention Systeme	☒ Besucher in Begleitung durch Mitarbeiter
☒ Einsatz von VPN bei Remote-Zugriffen	☒ Sorgfalt bei Auswahl des Wachpersonals
☒ Verschlüsselung von Datenträgern	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Verschlüsselung von Notebooks/Tablet (Windows)	☒ IT-Verfahren sicheres Passwort
☒ BIOS Schutz (separates Passwort)	☒ IT-Verfahren Löschen/Vernichten
☒ Überwachung externer Schnittstellen (USB)	☒ IT-Verfahren „Clean Desk“
☒ Automatische Desktopsperre	☒ Allg. Richtlinie Datenschutz und/oder Sicherheit
	☒ IT-Verfahren Mobile Device
	☒ Anleitung „Manuelle Desktopsperre“

3.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass

personenbezogene Daten bei der Verarbeitung, Nutzung und nach Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Aktenschredder	☒ Einsatz Berechtigungskonzept
☒ Externer Aktenvernichter (DIN 66399)	☒ Minimale Anzahl an Administratoren
☒ Physische Zerstörung von Datenträgern (DIN 66399)	☒ Datenschutztresor
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Verwaltung Benutzerrechte durch Administratoren
☒ Sicherung von Schnittstellen	

3.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Mandantenfähigkeit relevanter Anwendungen	☒ Festlegung von Datenbankrechten

3.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technische und organisatorische Maßnahmen unterliegen (Art.4 Nr. 5 DSGVO)

Aktuell keine entsprechenden Verarbeitungen.

4. Integrität

4.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von VPN	☒ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☒ Protokollierung der Zugriffe und Abrufe	
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
☒ Nutzung von Signaturverfahren	

4.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☒ Manuelle Kontrolle der Protokolle	☒ Vergabe von Rechten zur Eingabe, Änderung, Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	☒ Klare Zuständigkeiten für Löschungen

5. Verfügbarkeit und Belastbarkeit

5.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs
☒ Serverraumüberwachung (Temperatur, Feuchtigkeit)	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse.
☒ Serverraum klimatisiert	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ USV (unterbrechungsfreie Stromversorgung)	☒ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☒ Schutzsteckdosen Serverraum	☒ Getrennte Partitionen für Betriebssystem und Daten
☒ Datenschutztresor (S60DIS, S120DIS andere geeignete Normen mit Quelldichtung etc.)	
☒ RAID System / Festplattenspiegelung	
☒ Videoüberwachung Serverraum	
☒ Alarmmeldung bei unberechtigtem Zutritt zu dem Serverraum	
☒ Überspannungsschutz	

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

6.1. Datenschutzmaßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf / Berechtigung (Intranet)	☒ Interner Datenschutzbeauftragter
☒ Sicherheitszertifizierung nach ISO 22237	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet.
☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒ Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
	☒ Interner Informationssicherheitsbeauftragter
	☒ Die Datenschutz-Folgenabschätzung wird bei Bedarf durchgeführt (DSFA)
	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen vorhanden

6.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen
☒ Intrusion Prevention System (IPS)	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvor-fällen und Datenpannen

6.3. Datenschutzfreundliche Voreinstellungen

Privacy by design / privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	

☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

6.4. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln oder anderer Garantien
	☒ Schriftliche Weisungen (E-Mail, Ticket) an den Auftragnehmer
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☒ Regelung zum Einsatz weiterer Subunternehmer
	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

7. Gültigkeit und Dokumenten-Management

Dieses Dokument ist ab Freigabe gültig.

Der Eigentümer des Dokuments ist der Informationssicherheitsbeauftragte (ISB), der das Dokument mindestens einmal jährlich prüfen und ggf. aktualisieren muss.